

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xii
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xvi
1	INTRODUCTION	1
	1.1 Background of the Problem	1
	1.2 Statement of the Problem	3
	1.3 Aim	4
	1.4 Objectives of the Study	5
	1.5 Scope of the Study	5
	1.6 Significance of the Study	6
2	LITERATURE REVIEW	8
	2.1 Overview of Information Security	8
	2.2 Security in a Network-Centric Environment	9
	2.3 Definition of Web Service	10
	2.4 Security Standards and Technology	12
	2.4.1 Transport-Level Security: SSL	13
	2.4.2 XML Encryption	14
	2.4.3 XML Signature	14

2.4.4	XML Key Management Specification (XKMS)	15
2.4.5	Security Assertions Markup Language (SAML)	16
2.4.6	XML Access Control Markup Language (XACML)	17
2.4.7	X.509 Certificates	17
2.4.8	Web Services security specifications	18
2.4.9	Kerberos	21
2.5	Overview of Service Oriented Architecture (SOA)	21
2.5.1	Definition of Service Oriented Architecture (SOA)	22
2.5.2	Basic components of a SOA	24
2.5.3	Enterprise Service Bus	26
2.6	Understanding Enterprise SOA (ESOA)	27
2.6.1	The ESOA development lifecycle	30
2.7	S3: A Service-Oriented Reference Architecture	31
2.7.1	Operational Systems Layer	32
2.7.2	Service Component Layer	33
2.7.3	Services Layer	33
2.7.4	Business Process Layer	34
2.7.5	Consumer Layer	35
2.7.6	Integration Layer	35
2.7.7	Quality of Service Layer	36
2.7.8	Information Layer	37
2.7.9	Governance Layer	37
2.8	Service Oriented Modeling and architecture (SOMA)	38
2.8.1	Business modeling and transformation	40
2.8.2	Solution management	40
2.8.3	Identification phase	41
2.8.4	Specification phase	41
2.8.5	Realization phase	42
2.8.6	Implementation, deployment, and management phases	43
2.9	Understanding SOA security	43
2.9.1	Applying security at the message level	44
2.9.2	Converting Security into a Service	46
2.9.3	Declarative and Policy-based Security	48
2.10	Related works	48

2.10.1 SOA Security Framework for N C E	48
2.10.2 IBM SOA Security Reference Model	50
2.10.3 SOA Infrastructure Reference Model	51
2.11 Current ESOA security solutions and products	52
2.11.1 SOA Software Solutions	52
2.11.2 IBM SOA Security Solutions	54
2.11.3 Oracle SOA Security Solution	55
2.11.4 JBoss ESOA Platform	55
2.11.5 Vordel solution	56
2.11.6 Comparison of current solutions	59
2.12 Summary	60
3 RESEARCH METHODOLOGY	61
3.1 Research Design and Procedure	61
3.1.1 Literature Review	61
3.1.2 Analysis of Requirement	62
3.1.3 Design	62
3.1.4 Development	62
3.1.5 Verification	63
3.2 Instrumentation	65
3.3 Assumptions and Limitations	65
3.4 The Gantt chart of Research Activities	67
4 LOGICAL SECURITY FRAMEWORK FOR AN ESOA	69
4.1 ESOA security requirements	69
4.1.1 Identity	70
4.1.2 Trust management	71
4.1.3 Authorization	71
4.1.4 Audit	72
4.1.5 End-to-End Security	72
4.1.6 Privacy	73
4.1.7 Interoperability	73
4.1.8 Secure Configuration	74
4.1.9 Availability	74

4.1.10	Quality of Service	74
4.1.11	Secure Development	75
4.1.12	Assurance	75
4.1.13	Firewall	76
4.1.14	Service discovery	76
4.1.15	Security policy	77
4.1.16	Physical security	77
4.1.17	Time management	77
4.2	Logical Security Framework	78
4.2.1	Content Security Services	80
4.2.2	Compliance and Reporting	81
4.2.3	Identity and Access Services	81
4.2.4	Infrastructure Security Services	84
4.2.5	Privacy Service	85
4.2.6	Audit Service	86
4.2.7	Trust Management Service	86
4.2.8	Time Management Service	87
4.2.9	Security Policy Management Service	87
4.2.10	Governance and Risk Management	87
4.3	Security Service Oriented Reference Architecture (SSORA)	89
4.4	Logical Security Deployment Architecture of ESOA	91
4.5	SOA Security Solution Design	95
4.6	Conclusion	107
5	CASE STUDY: RAZAVI FINANCIAL INSTITUTE	108
5.1	Introduction to the case study	108
5.2	Business process	109
5.3	Solution overview	110
5.4	Service Modeling	110
5.4.1	Identification	111
5.4.2	Specification	113
6	IMPLEMENTATION	117
6.1	Apache Axis	117

6.1.1	Axis Architecture	118
6.1.2	Install Apache Axis	120
6.2	WSO2 Web Services Framework/PHP (WSO2 WSF/PHP)	123
6.2.1	Installing and Running on Microsoft Windows	124
6.3	Implementing case study	125
6.3.1	Customer Service	127
6.3.2	Proxy Service	128
6.3.3	Authentication Service	128
6.3.4	Portal	129
6.3.5	Secure Web Service Client	130
7	CONCLUSION AND FUTUER WORK	131
7.1	Conclusion	131
7.2	Contributions	133
7.3	Future work	134
	REFERENCES	135

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	The comparison of ESOA security solution	59
4.1	Security Services Standard	88
5.1	Goal-service model for the case study	112

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Security levels	10
2.2	XML Framework and non-XML Framework standards	13
2.3	Components of an XML Signature	15
2.4	Web Service security specifications	18
2.5	SOAP message security with WS-Security	19
2.6	SOA shift IT from an application-centric to service centric.	22
2.7	Elements of a SOA Stacks Presented by IBM	23
2.8	SOA components and operations	25
2.9	Enterprise Service Bus (ESB)	26
2.10	An ESOA framework presented by [23] .	28
2.11	The emerging ESOA infrastructure	29
2.12	The ESOA development lifecycle presented by SAP	30
2.13	Logical layers in Service Oriented Reference Architecture	32
2.14	Interactions in the integration layer	36
2.15	SOMA phases—a fractal model of software development.	38
2.16	SOMA Life-cycle high-level flow	39
2.17	The different envelope can be placed inside the main envelope	45
2.18	One of the possible ways in which a security service can work	47
2.19	Security service can be implemented as part of ESB.	47
2.20	Security framework for SOA presented by Catharina Candolin	49

2.21	IBM Security Reference Model	50
2.22	SOA Infrastructure Reference Model	51
3.1	Research Design and Procedure	63
3.2	Research Flow Chart	64
4.1	The Proposed Logical Security Framework for ESOA	80
4.2	End to End security in the SOA	81
4.3	Identity propagation in the SOA	83
4.4	Identity and Access Service framework	84
4.5	The six main layers of Service Oriented Reference Architecture	89
4.6	The proposed Security Service Oriented Reference Architecture	91
4.7	IBM Typical logical deployment architecture	92
4.8	The Proposed Logical Deployment Architecture of ESOA	94
4.9	The sequence diagram of ESOA Deployment Architecture	94
4.10	Decryption Service – sequence diagram	95
4.11	Reference Architecture for the Authentication Service	97
4.12	Authentication of browser-based user identity	97
4.13	Authentication of WS-Client request – sequence diagram	98
4.14	Use of SAML and XACML in Implementing ABAC	99
4.15	The proposed Service Routing Coordinator Architecture	100
4.16	Service Routing Coordinator Architecture – sequence diagram	101
4.17	STS Architecture	103
4.18	Security Token Service sequence diagram	104
4.19	Service-Oriented Audit Architecture	105
4.20	Security solution class diagram	106
4.21	The Complete Proposed ESOA Security Solution Design	106
5.1	A holistic business processes of RFI	109

5.2	Logical SOA deployment architecture for this case study	110
5.3	Identity and Access management	114
5.4	Complete security solution design for case study	116
6.1.	The Axis engine uses chains of handlers	119
6.2	The Tomcat localhost home page	121
6.3	The Apache Axis home page	121
6.4	The Axis Happiness page	122
6.5	WSDL list of Web Service	123
6.6	The sequence diagram of case study (web customer scenario)	126
6.7	The view of NetBeans and the location of services	127
6.7	The web based client to send username and password	127
6.8	The portal service main page	129

LIST OF ABBREVIATIONS

SOA	-	Service Oriented Architecture
ESOA	-	Enterprise Service Oriented Architecture
SOMA	-	Service Oriented Modeling and Architecture
XML	-	eXtensible Markup Language
WSDL	-	Web Service Description Language
UDDI	-	Universal description Discovery and Integration
SOAP	-	Simple Object Access Protocol
RFI	-	Razavi Financial Institute
MSIC	-	Mazan Salamat Insurance Co.
PKI	-	Public Key Infrastructure
SSL	-	Secure Socket Layer
MEP	-	Message Exchange Pattern
XKMS	-	XML Key Management Specification
SAML	-	Security Assertions Markup Language
XACML	-	XML Access Control Markup Language
WSDL	-	Web Security Policy Language
SSO	-	Single Sign On
ESB	-	Enterprise Service Bus
WBS	-	Work Breakdown Structure
GSM	-	Goal Service Modeling
SSORA	-	Security Service Oriented Reference Architecture

DMZ	-	Demilitarized Zone
DCS	-	Decryption Service
AZS	-	Authorization Service
ATS	-	Authentication Service
PS	-	Policy Service
CSS	-	Content Security Service
SRC	-	Service Routing Coordinator